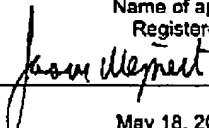I hereby certify that this correspondence is being I hereby certify sent
via facsimile to the United States Patent and Trademark Office at
facsimile no.: 571-273-8300 (Central number) on the below date:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
on May 18, 2006
_____
Date of Deposit

Jason M. Wejnert, Reg. No. 55,722
_____
Name of applicant, assignee or
Registered Representative

_____
Signature
May 18, 2006
_____
Date of Signature

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln. of: Busam et al.

Appln. No.:   09/955,665   Examiner: Tran, N. V.

Filed: September 19, 2001   Art Unit: 2151

For: Device-to-Device Network

Attorney Docket No: 11336/1166 (P00108US)

APPEAL BRIEF

Mail Stop Appeal Brief – Patent
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Appellant appeals from the decision of the examiner to the Board of Patent
Appeals and Interferences in the above-identified patent application. Appellant has filed
this Appeal Brief with the appropriate fee in accordance with 37 CFR § 41.37 and
§41.20(b)(2).

Real Party in Interest

The real party in interest is Harman Industries International, Incorporated,
a corporation having a place of business in Northridge, California.

Related Appeals and Interferences

The Appellant does not know of any related appeals or interferences.

Status of Claims

1.   Claims 1-24, 26, 28-43, 45, 47-57 are pending in the application.

2.   Claims 1-24, 26, 28-43, 45, 47-57 were finally rejected on Sept. 21, 2005.

3.   Appellant appeals the decision of the examiner finally rejecting claims 1-24, 26, 28-43, 45, 47-57.

Status of Amendments

All amendments have been entered, including the amendment subsequent to the September 21, 2005 final rejection made in a response dated December 21, 2005.

Summary of Claimed Subject Matter

The claims are directed to techniques for communicating data in a peer-to-peer network. In one implementation a request from a source device to access a network of devices is received. The network of devices includes one set of devices that have been authenticated or logged into the network under a particular identifier for those devices. The communication techniques determine with which devices the source device is authorized to access and communicate. In particular, the source device is allowed to communicate with the first set of devices when there is a correspondence between an identifier of the source device, and the particular identifier under which the first set of devices have been authenticated or logged into the network. In addition, the network includes a second set of devices that the source device is not authorized to access. Accordingly, an individual may connect to the network (e.g., with a laptop) and access other devices (e.g., an audio player) associated to that individual through a consistent identifier, while remaining unauthorized to access other devices associated with other individuals (e.g., because they have been authenticated under a different identifier).

Another feature includes searching for items on the first set of devices connected to the network and generating a playlist of items that exist on the first set of devices, where the items are located on different devices. Other features include attempting a second connection between a source device and a target device, via a proxy, if a first connection between the source device and target device is unsuccessful.

2

Grounds of Rejection to be Reviewed on Appeal

1. Whether Claims 1-4, 7, 9-12, 15-16, 18, 22-24, 28-29, 32-35, 37, 40-43, 47-48, 51-53, and 56-57 are unpatentable under 35 U.S.C. § 103(a) in view of *Vilhuber* (U.S. Patent No. 6,470,453) and *Huang* (U.S. Patent No. 6,571,245).

2. Whether Claims 5, 6, 8, 17, 19-21, 26, 30-31, 36, 38-39, 45, 49-50, and 54-55 are unpatentable under 35 U.S.C. § 103(a) over *Vilhuber* and *Huang* in view of *London* (U.S. Patent No. 6,061,734).

3. Whether Claim 13 is unpatentable under § 103(a) in view of *Vilhuber*, *Huang*, and *Dreke et al.* (U.S. Pat. No. 6,463,471).

4. Whether Claim 14 is unpatentable under § 103(a) in view of *Vilhuber*, *Huang*, *Dreke et al.*, and *Levy* (U.S. Pat. Pub. No. 2002-0052885).

The arguments below group the claims as follows:

Group 1: Claims 1-4, 7, 9-12, 18, 22, 28-29, 32-33, 37, 40-41, 47-48, and 51-52.

Group 2: Claims 15-16 and 34-35.

Group 3: Claim 23-24 and 42-43.

Group 4: Claim 53 and 56-57.

Group 5: Claim 5, 6, 8, 17, 19-21, 26, 30-31, 36, 38-39, 45, 49-50, and 54-55.

Group 6: Claim 13.

Group 7: Claim 14.

Argument

An obviousness analysis includes an assessment of the scope and content of the prior art. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). Obviousness is a legal conclusion based on underlying factual inquiries. The factual inquiries include: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) objective evidence of nonobviousness. *Graham*, 383 U.S. at 17-18. A successful assertion that a claim is obvious based on a combination of references requires a suggestion or motivation to combine the references. *WMS Gaming Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1355 (Fed. Cir. 1999). Furthermore, an obviousness rejection requires that the combined

3

prior art references teach or suggest all of the claim limitations. *CFMT, Inc. v. Yieldup Int'l Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003).

1. **Rejection of Claims** 1-4, 7, 9-12, 15-16, 18, 22-23, 28-29, 32-35, 37, 40-41, 47-48, and 51-53, and 56-57 **under §103(a).**

   a. **Group 1: Claims** 1-4, 7, 9-12, 18, 22, 28-29, 32-33, 37, 40-41, 47-48, and 51-52. The *Vilhuber-Huang* **combination does not teach or suggest the claimed data communication system with a first and second set of devices, determining that a source device is authorized to access a first set of devices based on an identifier, or the other features recited in the Group 1 claims.**

Claim 1 is directed to a method for communicating data including receiving a request from a source device to access a network of devices. The network of devices includes a first set of devices with an associated identifier, and a second set of devices that the source device is not authorized to access. The claimed method determines if the source device is authorized to access the first set of devices based on the source device's identifier. As claimed, the method determines whether the source device is authorized to access to the first set of devices based on a correspondence between an identifier of the source device and the associated identifier of the first set of devices.

The *Vilhuber-Huang* combination is directed to authenticating multiple connections to a network server which provides a virtual desktop in a virtual computing environment. The Final Office Action has asserted that the *Vilhuber-Huang* combination discloses the features of claim 1, including determining that the source device is authorized to access the first set of devices based on a correspondence between an identifier of the source device and an identifier associated with the first set of devices [*Huang*, fig. 13A-B and col. 14, l. 57- col. 15, l. 67]. Appellant respectfully disagrees.

Even assuming motivation to make the *Vilhuber-Huang* combination, the combination does not disclose a network in which a first set of devices uses a first identifier which is also associated with a source device, and a second set of devices that the source device is not authorized to access. Instead, in the *Vilhuber-Huang* combination, once the user is authorized to access the network access server 104

4

[*Huang*, Fig. 1], the user has access to the entire network system 108 [*Huang*, Fig. 1], including the network devices 114a-c [*Huang*, Fig. 1]. In addition, the *Vilhuber-Huang* combination requires a password login technique to access the network devices from a source device, and does not teach or disclose, as claimed, an identifier associated with any of the network devices themselves.

The Office Action admits that *Vilhuber* does not suggest or teach determining that the source device is authorized to access first set of devices based on a correspondence between an identifier of the source device and an identifier associated with the first set of devices. Instead, the Office Action alleges that *Huang* discloses determining that the source device is authorized to access a first set of devices based on a correspondence between an identifier of the source device and an identifier associated with the first set of devices. [Office Action mailed September 21, 2005, at 3]. Appellant respectfully disagrees.

Huang is directed to a password login technique for a client-server system to allow access to network devices from a source device. Once the source device is authenticated to access the network, the source device may access any of the network devices. *Huang* does not disclose how the devices and servers are connected or authenticated to the network. In particular, *Huang* does not disclose or teach authorizing a source device to access a first set of devices based on an identifier corresponding to an identifier associated with the first set of devices. *Huang* is silent on whether the first set of devices is authenticated or whether the first set of devices even has an associated identifier. Thus, a combination of *Vilhuber* and *Huang* also fails to teach or suggest the claimed subject matter.

The Office Action suggests that *Vilhuber* discloses at Col. 9, lines 8-27 a second set of devices that the source device is not authorized to access [*Id.* at 2]. However, this passage in Vilhuber refers to the source device being authorized to access the network of devices, rather than referring to a second set of devices that the source device may not access. Neither *Vilhuber* or *Huang* or their combination discloses or teaches a second set of devices that the source device is not authorized to access.

Claims 18, 28, 34, 37, and 47 also recite features of a network of devices that includes a first set of devices, which a source device is authorized to access, and which

5

have been authenticated or logged in based on an associated identifier, and a second set of devices, which the source device is not authorized to access. Accordingly, the *Vilhuber-Huang* combination does not teach or suggest the subject matter of these claims either. Appellant therefore respectfully requests the Board to reverse the decision of the Examiner rejecting the claims in Group 1 under §103(a).

> **b.   Group 2: Claims 15-16 and 34-35. The *Vilhuber-Huang* combination does not teach or suggest the claimed acts of identifying items on a first set of devices and creating a playlist of the items on the first set of devices, where the playlist includes items on different devices.**

Claims 15-16 and 34-35 are directed to a method and a processor readable storage device, respectively. The claims recite data communication features including determining that a source device is authorized to access a first set of devices based on a correspondence between a source device identifier and an identifier associated with the first set of devices. The claims identify items on the first set of devices and create a playlist of the items that exist on the first set of devices. The claims also recite that the playlist includes items on different devices.

As discussed in section 1a above, the *Vilhuber-Huang* combination does not disclose a network in which a first set of devices uses a first identifier which is also associated with a source device for access authorization, and a second set of devices that the source device is not authorized to access. In addition, the Office Action does not point to any disclosure in the *Vilhuber-Huang* combination that shows creating a *playlist*, or adding items to a playlist. Instead of a playlist (*i.e.*, a list of playable items that may be downloaded or streamed [specification, first paragraph page 8]), the asserted *Vilhuber-Huang* combination discloses authenticating a client-server network for a virtual desktop in a computer network. In the *Vilhuber-Huang* combination, the network architecture retrieves a static list of virtual desktop items and presents the list to the user after authentication [*Huang*, col. 4, ll. 31-39; col. 6, ll. 36-39]. The list identifies for the user the accessible applications and files for that user. [*Huang*, col. 2, ll. 51-52; col. 3, ll. 1-4]. It is respectfully submitted, however, that one of ordinary skill in the art

6

would not consider a generic list of accessible applications, files, and folders to be a *playlist*.

Accordingly, the asserted *Vilhuber-Huang* combination does not yield the subject matter present in Group 2 claims. Therefore, Appellant respectfully requests the Board to reverse the decision of the Examiner rejecting the claims in Group 2 under §103(a).

c.   Group 3: Claim 23-24 and 42-43. The asserted *Vilhuber-Huang* combination does not teach or suggest receiving a search request from a source device, sending the search request to the first set of devices; and receiving search results from the first set of devices, and other limitations in the Group 3 claims.

The claims in Group 3, Claims 23-24 and 42-43, recite methods for communicating data including receiving a search request from a source device, authorizing the source device to access a first set of devices based on a correspondence between a source device identifier and a first device set identifier, sending the search request to the first set of devices; and receiving search results from the first set of devices.

Again, as discussed in section 1a above, the *Vilhuber-Huang* combination does not disclose a network in which a first set of devices uses a first identifier which is also associated with a source device for access authorization, and a second set of devices that the source device is not authorized to access.

The Final Office Action also does not point to any disclosure in *Vilhuber* or *Huang* which addresses receiving a *search request* from a source device, sending a search request to the first set of devices, or receiving search results from the first set of devices. *Huang* discloses a search capability for a source device [*Huang*, Col. 10: 15-26], but the *Huang-Vilhuber* combination does not teach or disclose sending a search request to a first set of devices that are authorized for access based on a correspondence between an identifier of the source device and the associated identifier of the first set of devices, as recited by the claims of Group 3. Neither does the *Huang-Vilhuber* combination teach or disclose receiving search results from a first set of devices authorized for access by the source device. Regardless, as explained above, the *Huang-Vilhuber* combination fails to teach or disclose a first set of devices that the

7

source device is authorized to access based on a correspondence between a source device identifier and an identifier associate with the first set of devices.

Accordingly, Appellant respectfully requests withdrawal of the rejection of the claims in Group 3 under §103(a).

d. Group 4: Claims 53 and 56-57. The *Vilhiber-Huang* combination does not teach or suggest logging a first device into a network of devices using a first user identification, identifying the devices that are logged in to the network using the first user identification, and allowing the first device to communicate with the devices that are logged into the network using the first user identification, and not allowing the first device to communicate with the devices that are logged into the network using the second user identification recited in the Group 4 claims.

Claims 53 and 56-57 recite logging a first device into a network of devices using a first user identification, identifying the devices that are logged in to the network using the first user identification, and allowing the first device to communicate with the devices that are logged into the network using the first user identification, and not allowing the first device to communicate with the devices that are logged into the network using the second user identification.

The Final Office Action alleges that the *Vilhuber-Huang* combination discloses identifying the devices that are logged into the network using a first user identification, and authenticating the first device based on a first identification [*Vilhuber*, Col. 5:38-45]. The Final Office Action also alleges that *Vilhuber* discloses devices logged into the network using second user identifications. The Final Office Action admits that *Vilhuber* does not disclose or teach authorizing the first device to access the devices logged into the network using a first identifier. The Final Office Action alleges that *Huang* discloses authorizing a first device to access devices logged into the network using a first user identification [*Huang*, Col. 14:57-15:67]. Appellant respectfully disagrees.

As discussed above in the section on the claims in Group 1, the *Vilhuber-Huang* combination discloses a network-client architecture, in which devices are connected to a server that a source device is authorized to access. However, there is no suggestion

8

that the devices are authenticated based on an identifier when logged into the network, let alone based on the same identifier used for the source device. The *Vilhuber-Huang* combination also does not disclose or teach a second set of devices, or a second identifier used to log devices into the network. Thus, the *Vilhuber-Huang* combination also does not disclose or teach allowing a first device to communicate with the devices that are logged into the network using the first user identification, and not allowing the first device to communicate with the devices that are logged into the network using the second user identification, as required by claim 53.

Accordingly, Appellant respectfully requests withdrawal of the rejection of the claims in Group 4 under §103(a).

2.   Rejection of Group 5 claims: Claims 5, 6, 8, 17, 19-21, 26, 30-31, 36, 38-39, 45, 49-50, and 54-55 The *Vilhuber-Huang-London* combination does not teach or suggest receiving a request to search, forwarding the request to search from an intermediate entity to a first set of devices, performing searches at the first set of devices based on the request to search, attempting to provide results from the searches directly to said source device from the first set of devices via direct connections which bypass the intermediate entity, and providing the results from the searches to the source device from the first set of devices via the intermediate entity if the direct connections cannot be established.

Claims 5, 6, 8, 17, 19-21, 26, 30-31, 36, 38-39, 45, 49-50, and 54-55 stand rejected under 35 U.S.C. § 103(a) over *Vilhuber* and *Huang* in view of *London*. Claims 5 is directed to receiving, at an intermediate entity, a search request from a source device, forwarding the search request to a first set of devices, and performing searches at the first set of devices. Claim 5 also recites attempting to provide search results from the first set of devices to the source device through direct connections which bypass the intermediate entity, and providing the search results to the source device through the intermediate entity if a direct connection cannot be made. The Office Action suggests that the combination of *Vilhuber*, *Huang*, and *London* discloses an intermediate entity that can provide search results to a source device from a first set of devices via the intermediate entity if direct connections between the source device and the first set of

9

devices cannot be established [Figs. 6-7, col. 9, l. 17- col. 10, l. 48; col. 1, l. 12- col. 2, l. 65]. Assignee respectfully disagrees.

Even assuming motivation to combine the three references, the *Vilhuber-Huang-London* combination does not disclose: 1) performing searches at the first set of devices, 2) attempting to provide search results from the first set of devices to the source device through direct connections which bypass the intermediate entity, or 3) providing the search results to the source device through the intermediate entity if a direct connection cannot be made. Instead, the *Vilhuber-Huang-London* combination discloses authenticating a user connection through a peer server included in a client-server network server architecture. The *Vilhuber-Huang-London* combination forwards a request from a user E to a resource B after verifying that the user is authorized to access resource B, through a peer server and proxy server [*London* col. 9, l. 33-col 10, l. 7]. Connections between a user [i.e. source device] on one network must be routed through a proxy server to reach a device or resource [i.e., a first set of devices] on a network of other devices. Therefore, the *Vilhuber-Huang-London* combination does not disclose attempting to provide search results from the first set of devices to the source device through direct connections which bypass the intermediate entity, as claimed, because the only connections between the first set of devices and the source device are connections through an intermediate entity [the proxy server 606 or 711 in *London* Figs. 6-7]. Accordingly, Assignee respectfully requests withdrawal of the rejection. Claims 17, 19, 30, 36, 38, 49, and 54 recite corresponding features. Therefore, Assignee respectfully requests withdrawal of the rejections for Claims 17, 19, 30, 36, 38, 49, and 54.

Furthermore, Claim 6 is directed to connecting and authenticating a source device in a private network, where the source device has a private address and does not have a globally unique address, and where the target device has a globally unique address and is inaccessible via the Internet. The features of claim 6 allow devices within a device-to-device network to communicate with each other using a private address without having to assign a globally unique address, such as a TCP/IP address, and when the devices are not connected to the Internet. This eliminates the need for a central server to assign globally unique addresses or maintain a database of unique device addresses, thereby reducing server burden.

10

On the other hand, the *Vilhuber-Huang-London* combination discloses authenticating a user access to resources on a client-server network with a peer server to authenticate the user's connections to resources in the network, which may be connected through proxy servers [Figs. 6-7, col. 9, l. 17- col. 10, l. 48; col. 1, l. 12-col. 2, l. 65]. The *Vilhuber-Huang-London* combination does not disclose a source device in a private network, or that the source device has a private address and does not have a globally unique address, or that the target device has a globally unique address and is inaccessible via an Internet. The *Vilhuber-Huang-London* combination is silent on these features, and does not limit the source or target device address or connections in any way. Accordingly, the *Vilhuber-Huang-London* combination does not teach or suggest the features of claim 6, and Assignee respectfully requests withdrawal of the rejection of claim 6.

Claims 8, 20, 31, 39, 45, 50, and 55 further include the feature of attempting to establish a second connection from the target device to the source device; transferring an item using the second connection if the attempt to establish the second connection was successful; and transferring the item via a proxy if the attempt to establish the second connection was not successful. The claimed features allow a second attempt to transfer items from a target device to a source device if the first connection attempt is unsuccessful, through a second connection attempt. If the second connection attempt is unsuccessful, a proxy server is used to transfer the item. The *Vilhuber-Huang-London* combination does not disclose second connection attempts, transferring items using the second connection if the second connection attempt is successful, or transferring an item via a proxy if the second connection attempt is not successful. In fact, the *Vilhuber-Huang-London* combination does not address at all what happens when there is an unsuccessful connection attempt. Thus, even if the *Vilhuber-Huang-London* combination is made, the combination would not disclose all of the features in claims 8, 31, 39, 45, 50, and 55. Therefore, Assignee respectfully requests withdrawal of the rejection of claims 8, 31, 39, 45, 50, and 55

Claims 26 and 45 recite a method and a processor readable storage device. Claims 26 and 45 recite receiving, from a requesting device, a request to transfer an item residing on a target device. Claim 26 also recites attempting to establish a first

11

connection between the requesting device and the target device; transferring the item from the target device to the requesting device using the first connection if the attempt to establish the first connection was successful; sending a message to the target device via an intermediate device if the attempt to establish the first connection was not successful; receiving an attempt to establish a second connection, between the requesting device and the target device via a proxy, if the attempt to establish the first connection was not successful; and transferring the item using the second connection if the attempt to establish the second connection was successful.

The Final Office Action suggests that the combination of *Vilhuber*, *Huang*, and London discloses the limitations of the claims in Claims 26 and 45 [Figs. 6-7, col. 9, l. 17- col. 10, l. 48; col. 1, l. 12- col. 2, l. 65]. However, the Final Office action does not at all address the features of claims 26 and 45. While the Final Office action addresses certain features of claim 5, claims 26 and 45 include different features, such as transferring an item using a second connection if the attempt to establish the second connection was successful.

Even assuming motivation to combine the three references, the *Vilhuber-Huang-London* combination does not disclose: attempting to establish a second connection from the target device to the source device; transferring an item using the second connection if the attempt to establish the second connection was successful; and transferring the item via a proxy if the attempt to establish the second connection was not successful. The claimed features allow a second attempt to transfer items from a target device to a source device if the first connection attempt is unsuccessful, through a second connection attempt. If the second connection attempt is unsuccessful, a proxy server is used to transfer the item.

The *Vilhuber-Huang-London* combination discloses authenticating a user connection through a peer server included in a client-server network server architecture. The *Vilhuber-Huang-London* combination only discloses forwarding a request from a user E to a resource B through a peer server and proxy server [*London* col. 9, l. 33-col. 10, l. 7]. The *Vilhuber-Huang-London* combination does not disclose second connection attempts, transferring items using the second connection if the second connection attempt is successful, or transferring an item via a proxy if the second

12

connection attempt is not successful. In fact, the *Vilhuber-Huang-London* combination does not address at all what happens when there is an unsuccessful connection attempt, as specified in the method of Claim 26 and the processor readable storage device of claim 45.

Therefore, Appellant respectfully requests the Board to reverse the decision of the Examiner rejecting claims in Group 5 under §103(a).

3.   Rejection of Group 6 claim: Claim 13. The *Vilhuber-Huang-Dreke* combination does not teach or suggest establishing said network of devices without using a server.

Claim 13 stands rejected under § 103(a) over *Vilhuber* and *Huang* in view of *Dreke et al* (U.S. Patent No. 6,463,471). Claim 13 recites an additional step of establishing the network of devices without using a server. The Office Action suggests the *Vilhuber-Huang-Dreke* combination discloses establishing a network of devices without using a server [*Dreke et al.*, Fig. 3]. Assignee respectfully disagrees.

The *Vilhuber-Huang-Dreke* combination discloses a method for authenticating and maintaining a distributed network presence information server, in which the user first logs into a server where he may obtain a list of peers of interest. Fig. 3 of *Dreke et al.* actually shows a step in the process after the user logs into an Internet Presence Information Server (IPIS). The user must log into the server before accessing peers directly [*Dreke et al,.* Col. 3, l. 20- Col. 4, l. 22]. In other words, the *Vilhiber-Huang-Dreke* combination, even assuming motivation to make the combination, does not teach or suggest eliminating logging into a server before accessing peers in a device network. Thus, even if the *Vilhuber-Huang-Dreke* combination is made, the combination would not disclose all of the claimed features. Therefore, Assignee respectfully requests withdrawal of the rejection of claim 13.

4.   Rejection of Group 7 claim: Claim 14. The *Vilhuber-Huang-Dreke-Levy* combination does not teach or suggest broadcasting from first, second, and third devices; listening for other devices by the first, second, and third devices;

13

and establishing and authenticating connections between the first, second, and third devices.

Claim 14 stands rejected under § 103(a) as being unpatentable over *Vilhuber*, *Huang*, and *Dreke* in view of *Levy* (U.S. Patent Application Pub. No. 2002/0052885). Claim 14 recites broadcasting from first, second, and third devices; listening for other devices by the first, second, and third devices; and establishing and authenticating connections between the first, second, and third devices. The features of claim 14 allow devices in a device-to-device network to broadcast their presence, and establish a network without requiring an intermediate server to connect the devices. The Office Action suggests the *Vilhuber-Huang-Dreke-Levy* combination discloses all the features of claim 14 [Office Action mailed September 21, 2005, at 10]. Assignee respectfully disagrees.
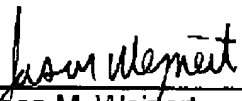
The *Vilhuber-Huang-Dreke-Levy* combination discloses a distributed network of devices using auxiliary data embedded in files to enhance file sharing systems. The cited portion of *Levy* [*Levy*, page 3, paragraph 0033] refers to computers broadcasting their event logs to each other. For example, *Levy* discloses "[i]n distributed systems where no central server is involved, the event logs [of file transfers] can be stored on computers in the file sharing network (or a subset of the computers), and composite event logs can be compiled by having the computers broadcast their event logs to each other. Each computer, in this approach, could maintain a copy of the event log, which is synchronized upon each broadcast operation." [*Levy*, page 3, paragraph 0033]. Thus, the *Vilhuber-Huang-Dreke-Levy* combination does not teach or suggest establishing and authenticating connections based on device-to-device broadcasts. Instead, the *Vilhuber-Huang-Dreke-Levy* combination simply broadcasts log files to various computers on the network. Accordingly, Assignee respectfully requests the Examiner to withdraw the rejection of Claim 14.

Conclusion

Appellant respectfully submits that the inventions defined in claims 1-24, 26, 28-43, 45, 47-57 are patentable in view of any combination of the cited references.

14

Appellant therefore requests reversal of all of the pending rejections asserted in the Final Office Action.

Respectfully submitted,

Jason M. Wejnert
Registration No. 55,722
Attorney for Appellant

BRINKS HOFER GILSON & LIONE
P.O. BOX 10395
CHICAGO, ILLINOIS 60610
(312) 321-4200

15

Claim Appendix - Pending claims 1-24, 26, 28-43, 45, 47-57

1.   A method for communicating data, comprising the steps of receiving a request from a source device to access a network of devices, said network of devices includes a first set of devices, which said source device is authorized to access, and which have been authenticated based on an associated identifier, and a second set of devices, which said source device is not authorized to access, said first set of devices being distributed across a global network;

determining that said source device is authorized to access said first set of devices based on a correspondence between an identifier of said source device and said associated identifier; and

responsive to said determining step, allowing communication between said source device and said first set of devices, and not allowing communication between said source device and said second set of devices.

2.   A method according to claim 1, wherein:

said identifier associated with said source device comprises a first user identification;

said first set of devices use said first user identification; and

said second set of devices do not use said first user identification.

3.   A method according to claim 2, further comprising the step of:

authenticating said first source device based on said first user identification and a first password, said step of allowing is performed in response to said step of authenticating.

4.   A method according to claim 1, wherein said step of allowing communication includes the steps of:

transmitting a search request to said first set of devices;

performing searches at said first set of devices based on said search request; and

providing results from said searches.

16

5. A method according to claim 1, wherein said step of allowing communication includes the steps of:

receiving, at an intermediate entity, and from said source device, a request to search;

forwarding said request to search from said intermediate entity to said first set of devices;

performing searches at said first set of devices based on said request to search;

attempting to provide results from said searches directly to said source device from said first set of devices via direct connections which bypass said intermediate entity; and

providing said results from said searches to said source device from said first set of devices via said intermediate entity if said direct connections cannot be established, said intermediate entity performs said step of receiving a request to access a network of devices.

6. A method according to claim 1, wherein said step of allowing communication includes the steps of:

transmitting a search request from said source device to a target device, which belongs to said first set of devices;

performing a search at said target device based on said search request; and

providing results from said search from said target device to said source device via a connection between said source device and said target device, said source device via a connection between said source device and said target device, said source device is in a private network, said source device has a private address and does not have a globally unique address, said target device has a globally unique address and is inaccessible via an Internet.

7. A method according to claim 1, wherein said step of allowing communication includes the steps of:

transmitting a search request from said source device to a target device which belongs to said first set of devices;

17

performing a search at said target device based on said search request; and

providing results from said search from said target device to said source device via a connection between said source device and said target device, said source device is behind a firewall.

8.   A method according to claim 1, wherein said step of allowing communication includes the steps of:

attempting to establish a first connection from said source device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

sending a message to said target via an intermediate device if said attempt to establish said first connection was not successful;

attempting to establish a second connection from said target device to said source device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

9.   A method according to claim 1, wherein:

said step of allowing communication includes transferring items, streaming items, searching for items, and viewing a list of items.

10.   A method according to claim 1, wherein:

said step of allowing communication includes sending a command from said a source device to one or more devices of said first set of devices.

11.   A method according to claim 1, wherein:

said step of allowing communication includes sending a command from said a source device to an intermediate server and forwarding said command from said intermediate server to one or more devices of said first set of devices.

18

12. A method according to claim 1, wherein said step of allowing communication includes the steps of:

creating a playlist; and

adding items to said playlist, said items include a first item from a first device and a second item from a second device, said first device and said second device are not on a common LAN.

13. A method according to claim 1, further comprising the step of:

establishing said network of devices without using a server.

14. A method according to claim 13, wherein said step of establishing includes the steps of:

broadcasting from a first device;

listening for other devices, performed by said first device;

broadcasting from a second device;

listening for other devices, performed by said second device;

establishing a connection between said second device and said first device;

authenticating said first device and said second device;

broadcasting from a third device;

listening for other devices, performed by said third device;

establishing a connection between said second device and said third device;

authenticating said second device and said third device;

establishing a connection between said third device and said first device; and

authenticating said first device and said third device.

15. A method for communicating data, comprising the steps of:

receiving a request from a source device to access a network of devices, said network of devices includes a first set of devices, which said source device is authorized to access, and which have been authenticated based on an associated

19

identifier, and a second set of devices, which said source device is not authorized to access;

determining that said source device is authorized to access said first set of devices based on a correspondence between an identifier of said source device and said associated identifier;

responsive to said determining step, identifying items on said first set of devices; and

responsive to said step of identifying said items, creating a playlist of said items on said first set of devices, said playlist includes items on different devices.

16.   A method according to claim 15, wherein:
said creating a playlist comprises creating a playlist of items on different types of devices.

17.   A method according to claim 15, wherein said step of identifying items includes the steps of:

receiving a request at an intermediate entity from said a source device to search;

forwarding said request to search from said intermediate entity to said first set of devices;

performing searches at said first set of devices based on said search request;

attempting to provide results from said searches directly to said source device from said first set of devices via direct connections which bypass said intermediate entity; and

providing said results from said searches to said source device from said first set of devices via said intermediate entity if said direct connections cannot be established.

18.   A method of communicating data, comprising the steps of:
logging a first device into a network of devices using a first user identification, said network of devices includes devices logged into said network using

20

said first user identification and devices logged in to said network using one or more other user identifications, said one or more other user identifications include a second user identification;

identifying said devices that are logged in to said network using said first user identification; and

responsive to said step of identifying allowing said first device to communicate with said devices that are logged into said network using said first user identifications and not allowing said first device to communicate with said devices that are logged in to said network using said second user identification.

19. A method according to claim 18, wherein said step of allowing said first device to communicate includes the steps of:

receiving a request at an intermediate entity from a requesting device to search, said requesting device is logged into said network using said first user identification;

forwarding said request to search from said intermediate entity to said devices that are logged in to said network using said first user identification;

performing searches at said devices that are logged in to said network using said first user identification based on said request;

attempting to provide results from said searches directly to said requesting device from said devices that are logged in to said network using said first user identification via direct connections which bypass said intermediate entity; and

providing said results from said searches to said first device from said devices that are logged in to said network using said first user identification via said intermediate entity if said direct connections cannot be established.

20. A method according to claim 18, wherein said step of allowing said first device to communicate includes the steps of:

attempting to establish a first connection from said first device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

21

sending a message to said target via an intermediate device if said attempt to establish said first connection was not successful, said intermediate entity performs said step of receiving a request to access a network;

attempting to establish a second connection from said target device to said first device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

21. A method according to claim 18, wherein:

said step of allowing said first device to communicate includes sending a command from said first device to an intermediate server; and

forwarding said command from said intermediate server to one or more of said devices that are logged in to said network using said first user identification.

22. A method according to claim 18, wherein said step of allowing said first device to communicate includes the steps of creating a playlist; and

adding items to said playlist, said items include a first item from said first device and a second item from a second device, said first device and said second device are not on a common LAN, said second device is logged in to said network using said first user identification.

23. A method of communicating data, comprising the steps of:

receiving a search request from a source device;

identifying a first set of devices, in a network of devices, wherein the source device is authorized to access the first set of devices, and the first set of devices have been authenticated based on an associated identifier, and wherein said identifying is based on a correspondence between an identifier of said source device and said associated identifier;

22

responsive to the identifying step, accessing the a first set of devices, said network of devices also includes a second set of devices which said source device is not authorized to access;

sending the search request to said first set of devices; and

receiving search results from said first set of devices.

24.   A method according to claim 23, wherein:

said step of sending includes sending said search request to a server for forwarding to said first set of devices; and

said step of receiving search results includes receiving said search results at said source device via direct connections, if direct connections between said source device and said first set of devices, which bypass the server, can be established;

wherein an attempt is made to establish said direct connections; and

said step of receiving search results includes receiving said search results at said source device via said server, if said direct connections cannot be established.

26.   A method for communicating data, comprising the steps of:

receiving, from a requesting device, a request to transfer an item residing on a target device;

attempting to establish a first connection, between said requesting device and said target device, in response to said step of receiving;

transferring said item from said target device to said requesting device using said first connection if said attempt to establish said first connection was successful;

sending a message to said target device via an intermediate device if said attempt to establish said first connection was not successful;

receiving an attempt to establish a second connection, between said requesting device and said target device via a proxy, if said attempt to establish said first connection was not successful; and

transferring said item using said second connection if said attempt to establish said second connection was successful.

23

28.   One or more processor readable storage devices for storing processor readable code, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving a request from a source device to access a network of devices, said network of devices includes a first set of devices, which said source device is authorized to access, and which have been authenticated based on an associated identifier, and a second set of devices, which said source device is not authorized to access; said first set of devices being distributed across a global network;

determining that said source device is authorized to access said first set of devices based on a correspondence between an identifier of said source device and said associated; and

responsive to said determining step, allowing communication between said source device and with said first set of devices, and not allowing communication between said source device and said second set of devices.

29.   One or more processor readable storage devices according to claim 28, wherein:

said identifier associated with said source device comprises said a first user identification;

said first set of devices use said first user identification; and

said second set of devices do not use said first user identification.

30.   One or more processor readable storage devices according to claim 28, wherein said step of allowing communication includes the steps of:

receiving, at an intermediate entity, and from said source device, a request to search;

forwarding said request to search from said intermediate entity to said first set of devices;

performing searches at said first set of devices based on said request to search;

24

attempting to provide results from said searches directly to said source device from said first set of devices via direct connections which bypass said intermediate entity; and

providing said results from said searches to said source device from said first set of devices via said intermediate entity if said direct connections cannot be established.

31. One or more processor readable storage devices according to claim 28, wherein said step of allowing communication includes the steps of:

attempting to establish a first connection from said a source device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

sending a message to said target device via an intermediate device if said attempt to establish said first connection was not successful, said intermediate entity performs said step of receiving a request to access a network;

attempting to establish a second connection from said target device to said source device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

32. One or more processor readable storage devices according to claim 28, wherein:

said step of allowing communication includes sending a command from said a source device to an intermediate server and forwarding said command from said intermediate server to one or more devices of said first set of devices.

33. One or more processor readable storage devices according to claim 28, wherein said step of allowing communication includes the steps of:

creating a playlist; and

25

adding items to said playlist, said items include a first item from a first device and a second item from a second device, said first device and said second device are not on a common LAN.

34. One or more processor readable storage devices for storing processor readable code, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving a request from a source device to access a network of devices, said network of devices includes a first set of devices, which said source device is authorized to access, and which have been authenticated based on an associated identifier, and a second set of devices, which said source device is not authorized to access;

determining that said source device is authorized to access said first set of devices based on a correspondence between an identifier of said source device and said associated identifier;

responsive to said determining step, identifying items on said first set of devices; and

responsive to said step of identifying said items, creating a playlist of said items on said first set of devices, said playlist includes items on different devices.

35. One or more processor readable storage devices according to claim 34, wherein:

said creating a playlist comprises creating a playlist of items on different types of devices.

36. One or more processor readable storage devices according to claim 34, wherein said step of identifying items includes the steps of:

receiving a request at an intermediate entity from said a source device to search;

forwarding said request to search from said intermediate entity to said first set of devices;

26

performing searches at said first set of devices based on said search request;

attempting to provide results from said searches directly to said source device from said first set of devices via direct connections which bypass said intermediate entity; and

providing said results from said searches to said source device from said first set of devices via said intermediate entity if said direct connections cannot be established, said intermediate entity performs said step of receiving a request to access a network of devices.

37.   One or more processor readable storage devices for storing processor readable code, said processor readable code for programming one or more processors to perform a method comprising the steps of:

logging a first device into a network of devices using a first user identification, said network of devices includes devices logged into said network using said first user identification and devices logged in to said network using one or more other user identifications, said one or more other user identifications include a second user identification;

identifying said devices that are logged in to said network using said first user identification; and

responsive to said step of identifying, allowing said first device to communicate with said devices that are logged into said network using said first user identification and not allowing said first device to communicate with said devices that are logged in to said network using said second user identification.

38.   One or more processor readable storage devices according to claim 37, wherein said step of allowing said first device to communicate includes the steps of:

receiving a request at an intermediate entity from said first device to search;

forwarding said request to search from said intermediate entity to said devices that are logged in to said network using said first user identification;

27

performing searches at said devices that are logged in to said network using said first user identification based on said request to search;

attempting to provide results from said searches directly to said first device from said devices that are logged in to said network using said first user identification via direct connections which bypass said intermediate entity; and

providing said results from said searches to said first device from said devices that are logged in to said network using said first user identification via said intermediate entity if said direct connections cannot be established.

39. One or more processor readable storage devices according to claim 37, wherein said step of allowing said first device to communicate includes the steps of:

attempting to establish a first connection, from said first device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

sending a message to said target via an intermediate device if said attempt to establish said first connection was not successful, said intermediate device said step of receiving a request to access a network;

attempting to establish a second connection from said target device to said source device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

40. One or more processor readable storage devices according to claim 37, wherein:

said step of allowing said first device to communicate includes sending a command from said first device to an intermediate server and forwarding said command from said intermediate server to one or more of said devices that are logged in to said network using said first user identification.

28

41. One or more processor readable storage devices according to claim 37, wherein said step of allowing said first device to communicate includes the steps of:

creating a playlist; and

adding items to said playlist, said items include a first item from said first device and a second item from a second device, said first device and said second device are not on a common LAN, said second device is logged in to said network using said first user identification.

42. One or more processor readable storage devices for storing processor readable code, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving a search request from a source device;

identifying a first set of devices, in a network of devices, wherein the source device is authorized to access the first set of devices, and the first set of devices have been authenticated based on an associated identifier, and wherein said identifying is based on a correspondence between an identifier of said source device and said associated identifier;

responsive to a identifying step, accessing the first set of devices, said network of devices also includes a second set of devices which said source device is not authorized to access;

sending the search request to said first set of devices; and

receiving search results from said first set of devices.

43. One or more processor readable storage devices according to claim 42, wherein:

said step of sending includes sending said search request to a server for forwarding to said first set of devices; and

said step of receiving search results includes receiving said search results at said source device via direct connections, if direct connections between said source device and said first set of devices, which bypass the server, can be established; wherein an attempt is made to establish said direct connections; and

29

said step of receiving search results includes receiving said search results at said source device via said server, if said direct connections cannot be established.

45. One or more processor readable storage devices for storing processor readable code, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving, from a requesting device, a request to transfer an items residing on a target device;

attempting to establish a first connection, between said requesting device and said target device, in response to said step of receiving;

transferring said item from said target device to said requesting device using said first connection if said attempt to establish said first connection was successful;

sending a message to said target device via an intermediate device if said attempt to establish said first connection was not successful;

receiving an attempt to establish a second connection, between said requesting device and said target device via a proxy, if said attempt to establish said first connection was not successful; and

transferring said item using said second connection if said attempt to establish said second connection was successful.

47. An apparatus for communicating data, comprising:

a communication interface; and

one or more processors, in communication with said communication interface, said one or more processors perform a method comprising the steps of:

receiving a request from a source device to access a network of devices, said network of devices includes a first set of devices, which said source device is authorized to access, and which have been authenticated based on an associated identifier, and a second set of devices, which said source device is not authorized to access, said first set of devices being distributed across a global network,

30

determining that said source device is authorized to access identifying said first set of devices based on a correspondence between an identifier of said source device and said associated identifier; and

responsive to said determining step, allowing communication between said source device and said first set of devices, and not allowing communication between said source device and said second set of devices.

48. An apparatus according to claim 47, wherein:

said identifier associated with said source device comprises a first user identification;

said first set of devices use said first user identification; and

said second set of devices do not use said first user identification.

49. An apparatus according to claim 47, wherein said step of allowing communication includes the steps of:

receiving, at an intermediate entity, and from said source device, a request to search;

forwarding said request to search from said intermediate entity to said first set of devices;

performing searches at said first set of devices based on said request to search;

attempting to provide results from said searches directly to said source device from said first set of devices via direct connections which bypass said intermediate entity; and

providing said results from said searches to said source device from said first set of devices via said intermediate entity if said direct connections cannot be established, said intermediate entity performs said step of receiving a request to access a network of devices.

50. An apparatus according to claim 47, wherein said step of allowing communication includes the steps of:

31

attempting to establish a first connection from said a source device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

sending a message to said target device via an intermediate device if said attempt to establish said first connection was not successful, said intermediate entity performs said step of receiving a request to access a network;

attempting to establish a second connection from said target device to said source device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

51. An apparatus according to claim 47, wherein:

said step of allowing communication includes sending a command from said a source device to an intermediate server and forwarding said command from said intermediate server to one or more devices of said first set of devices.

52. An apparatus according to claim 47; wherein said step of allowing communication includes the steps of:

creating a playlist; and

adding items to said playlist, said items include a first item from a first device and a second item from a second device, said first device and said second device are not on a common LAN.

53. An apparatus for communicating data, comprising:

a communication interface; and

one or more processors in communication with said communication interface, said one or more processor perform a method comprising the steps of:

logging a first device into a network of devices using a first user identification, said network of devices includes devices logged into said network using

32

said first user identification and devices logged in to said network using one or more other user identifications, said one or more other user identifications include a second user identification,

identifying said devices that are logged in to said network using said first user identification, and

responsive to said step of identifying, allowing said first device to communicate with said devices that are logged into said network using said first user identification, and not allowing said first device to communicate with said devices that are logged into said network using said second user identification.

54. An apparatus according to claim 53, wherein said step of allowing said first device to communicate includes the steps of:

receiving a request from said first device at an intermediate entity to search;

forwarding said request to search from said intermediate entity to said devices that are logged in to said network using said first user identification;

performing searches at said devices that are logged in to said network using said first user identification based on said request;

attempting to provide results from said searches directly to said first device from said devices that are logged in to said network using said first user identification via direct connections which bypass said intermediate entity; and

providing said results from said searches to said first device from said devices that are logged in to said network using said first user identification via said intermediate entity if said direct connections cannot be established.

55. An apparatus according to claim 53, wherein said step of allowing said first device to communicate includes the steps of:

attempting to establish a first connection from said first device to a target device;

transferring an item using said first connection if said attempt to establish said first connection was successful;

33

sending a message to said target device via an intermediate device if said attempt to establish said first connection was not successful, said intermediate entity performs said step of receiving a request to access a network;

attempting to establish a second connection from said target device to said source device;

transferring said item using said second connection if said attempt to establish said second connection was successful; and

transferring said item via a proxy if said attempt to establish said second connection was not successful.

56. An apparatus according to claim 53, wherein:

said step of allowing said first device to communicate includes sending a command from said first device to an intermediate server and forwarding said command from said intermediate server to one or more of said devices that are logged in to said network using said first user identification.

57. An apparatus according to claim 53, wherein said step of allowing said first device to communicate includes the steps of:

creating a playlist; and

adding items to said playlist, said items include a first item from said first device and a second item from a second device, said first device and said second device are not on a common LAN, said second device is logged in to said network using said first user identification.

34

Evidence Appendix

The Appellant has not submitted any evidence under 37 CFR §1.130, 1.131 or 1.132, nor has the Examiner entered any evidence on which the Appellant relies. Therefore, no copies of such evidence are submitted.

35

Related Proceedings Appendix

The Appellant does not know of any related appeals or interferences. Therefore, no copies of decisions in any such proceedings are submitted.

36